Fault Classification and Fault Tolerance Metrics for NoC

By Tassawer Amin
Advisor Michael Imhof
Agenda

- Motivation
- Reliability
  - Variability
  - Transistor performance degradation (Aging)
  - Soft errors (Transient Faults)
  - Intermittent faults
- Fault Tolerance
  - Network on chip (NoC)
  - Traditional Fault tolerance metrics
  - Fault tolerance metrics for NoC
Motivation

SSI = Small scale Integration
MSI = Medium scale Integration
VLSI = Very large scale integration
ULSI = Ultra large level integration
GSI = Giga scale integration
Motivation

More Transitors
• More computing power

More Internal capacitance
• More gate delays

Leakage current
• Power dissipation
• Variability

Reliability Issues
• Soferrors
• Intermittent faults

Wilman Tsai, Robert Chau. *Integration of Metal gate High k Dielectrics to Extend Transistor Scaling*, 2004

2014, 2-5 billion transistors with 10-13 nm gate on a chip area of 500-700 mm²
Motivation

Reliability
- Variability
- Transistor performance degradation (Aging)
- Soft errors (Transient Faults)
- Intermittent faults

Fault Tolerance
- Network on chip (NoC)
- Traditional Fault tolerance metrics
- Fault tolerance metrics for NoC
Reliability

- Variability
  - Random dopant fluctuations
  - Sub wavelength lithography
  - Heat flux
- Performance degradation
- Soft errors (Transient faults)
- Intermittent faults
Variability

- Types
  - Physical (Static)
    - During fabrication process
      - Incorrect dimensions
      - Difference in effective channel length
  - Environmental (Dynamic)
    - Unpredictability of environmental conditions
      - Change in chip temperature
      - Change in power supply voltage

- Causes of variation
  - Random dopant fluctuations
  - Sub wavelength lithography
  - Heat flux
Random dopant fluctuations

Why
- Control threshold voltage

Problems
- Deletion of Impurity atoms
- Different dopant concentrations on each edge

Shekhar, Borkar. "Designing Reliable System From Unreliable Components." 2005
Sub wavelength lithography

- Why
  - Patterning transistors during fabrication
- Problems
  - Line edge roughness
  - Corner rounding etc.

Kelin Kuhn, Chris Kenyon—Managing Process Variation in Intel’s 45nm CMOS Technology, 2004

Heat Flux

- Why
  - Higher activity rate of specific parts

- Problems
  - Increase in system temperature
  - Hot spots
  - Higher sub threshold leakage

Reliability

- Variability
- **Performance degradation (Aging)**
- Soft errors (Transient faults)
- Intermittent faults
Performance Degradation (Aging)

Why
- Excessive Use
- Hot carrier based Degradation

Problems
- Decline in performance leading to failure

Solutions
- Burn in Test
- Light doped source drain

Shekhar, Borkar. "Designing Reliable System From Unreliable Components." 2005
Reliability

- Variability
- Performance degradation (Aging)
- **Soft errors (Transient faults)**
- Intermittent faults
Soft errors (Transient Faults)

- Why
  - Alpha particles emitted from the uranium impurities
  - Isotopic boron used to form Insulation layer
  - Ions produced by high energy neutron reaction with silicon nuclei

Occurrence rate varies with altitude

A complex system of 1-megagate SRAM-based FPGA devices would on average, exhibit a functional failure every 11 months. This is a best-case number, this same system, if deployed in London or Denver, would fail every 3 to 7 months.

A system of similar complexity, if used in an aircraft or other high altitude environments, would have a SER that is 100-800 times worse, and a functional failure would occur every 12 to 3 hours.

“Neutrons from Above” Soft Error Rates, Actel
Soft errors (Transient Faults)

- Memory elements are much more sensitive to soft errors
  - DRAM
  - Latches/Flip flops
    - Becoming bigger threat
      - Difficult to detect as period of vulnerability varies

\[ \text{SET} = \text{Single event transient} \]
\[ \text{SEU} = \text{Single event upset} \]

Baumann, Robert. "Soft errors in advanced computer systems. 2005
Soft errors (Transient Faults)

- Solutions
  - Parity bit Checking
  - Error detecting and correcting Codes

Shekhar, Borkar. "Designing Reliable System From Unreliable Components." 2005
Reliability

- Variability
- Performance degradation (Aging)
- Soft errors (Transient faults)
- Intermittent faults
Intermittent Errors

- Why
  - Temperature and voltage fluctuations
  - In process wear-out (unstable hardware)
- Occurs in burst at the same location
- System produces errors until the fault is active
- Occurs 10-30 times as often as permanent faults
- Hard to find in very large and complex systems
Intermittent Errors

- Prevention Methods
- Example Multi Core system

G.S. Wells, P.M. Chakraborty, “Adapting to Intermittent Faults in Future Multi core Systems. 2007

Fault Tolerance and Fault Tolerance Metrics for NoC
Motivation
Reliability
Fault Tolerance
- Network on chip (NoC)
- Traditional Fault tolerance metrics
- Fault tolerance metrics for NoC
Agenda

- Motivation
- Reliability
- Fault Tolerance
  - *Network on chip (NoC)*
  - Traditional Fault tolerance metrics
  - Fault tolerance metrics for NoC
Network On Chip (NoC)

- Large number of resources and their interconnections
  - Bus based approach using in SoC (arbiter)
    - Scalability issues
    - Higher bandwidth requirements (multimedia applications)
    - Wiring delay due to increased capacitance
Network On Chip (NoC)

SW = Switches
NI = Network Interface
PE = Processing elements

## Network On Chip (NoC)

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical layer</td>
<td>• Length of wires required to connect resources to switches</td>
</tr>
<tr>
<td>Data link layer</td>
<td>• Protocol to transmit resource→ switch / switch → switch communication</td>
</tr>
<tr>
<td>Network layer</td>
<td>• How to transmit packets over the network</td>
</tr>
<tr>
<td></td>
<td>• Routing decisions</td>
</tr>
<tr>
<td>Transport layer</td>
<td>• End → End error recovery and flow control</td>
</tr>
<tr>
<td>Session layer</td>
<td>• Establishing, Managing and Termination of End → End Connections</td>
</tr>
<tr>
<td>Presentation layer</td>
<td>• Encryption of data to be sent</td>
</tr>
<tr>
<td>Application Layer</td>
<td>• All application specific tasks</td>
</tr>
</tbody>
</table>
Agenda

- Motivation
- Reliability
- Fault Tolerance
  - Network on chip (NoC)
  - *Traditional Fault tolerance metrics*
  - Fault tolerance metrics for NoC
Fault tolerance

- **Failure Rate**
  - expected number of failures a system can suffer during a specific time period

- **Mean time to failure**
  - Estimated time till which the system will keep on functioning correctly before the first error occurs

- **Mean time between failure (MTBF)**
  \[
  MTBF = \frac{\text{Total Operating time}}{\text{Number of failures encountered}}
  \]

- **Mean time to recover (MTTR)**
  \[
  MTTR = \frac{\text{Time Spent for repair}}{\text{Number of repairs}}
  \]

- **Availability**
  \[
  \text{Availability} = \frac{MTBF}{MTBF + MTTR} \times 100\%
  \]
Fault tolerance

Detect/Repair

Application level (Application layer)

Detect/Repair

End-End/Switch-Switch (Transport Layer)

Detect/Repair

Flit/Packet level (Data Link layer)

Detect/Repair

Layout and Device level (Physical layer)

Faults

Increasing detection / recovery time
Traditional Fault tolerance Metrics

- Fault tolerance metrics
  - Measure the system design in terms of its reliability, availability, safety, performance, maintainability and dependability against its failure rate, MTBF (Mean time between failure) and MTTR (Mean time to recover).

  - Not suitable for NoC
    - MTBF misinterprets NoC ability of rapid recovery in case of failure
    - Tells us average values which does not satisfy NoC guaranteed latency and throughput in case of failure
Agenda

- Motivation
- Reliability
- Fault Tolerance
  - Network on chip (NoC)
  - Traditional Fault tolerance metrics
  - Fault tolerance metrics for NoC
Comprehensively analyze the effectiveness of each fault tolerance method in context of specific NoC implementation.

Use of combination of different fault tolerance methods at different communication layers.

Faults can be categorized by their respective type, source, frequency of occurrence and their significant impact on the system.
Fault tolerance Metrics for NoC

Avoidance
- Reduce the chances for the error to occur
  - Data redundancy
    - Add extra information
  - Hardware redundancy
    - Add extra hardware
  - Time redundancy
- Increased latency
  - Extra time required by the avoidance mechanism is added to the total latency to transport data
Detection

- Fault Occurs
  - No error correcting mechanism implanted at upper level
  - correction failed
- Early detection to initiate recovery in case of fatal errors
- End $\rightarrow$ End
- Switch $\rightarrow$ Switch
Fault tolerance Metrics for NoC

- Containment
  - limiting the impact of fault
  - Stop propagation
  - Fault Containment regions

![Fault Containment Region](image)
Fault tolerance Metrics for NoC

- Isolation
  - Eliminate the use of faulty processing elements
  - Physical level (Permanent)
    - Disconnecting faulty NoC Component
  - Upper layers
    - Dropping faulty data packets
Fault tolerance Metrics for NoC

- Recovery
  - Providing means to recover from the failure
  - Recovery time evaluation
    - Area and power consumption
  - Physical layer
    - Providing hardware correction
  - Upper layers
    - Retransmission requests
Thanks alot for your attention